GWR COMMENTS ON THE
30 OCT CIA DCID 1/16 RESPONSE

I have reviewed the subject CIA response and Lara's Comments thereon. In general I agree with Lara's comments. My comments are as follows:

Position	Comment
1. DCID blends policy and implementation.	Reduction of the DCID to only general statements of policy would defeat the objective of uniformity of interepretation. It is too late in the process to change the general approach completely. If CIA has specific suggestions they should present them.
2. Accreditation authority should be delegated further (to DD's at CIA)	As stated in CIA's position 5, accreditation is an assumption of risk. The current draft makes a reasonable compromise on the varying positions of the Community as to what level this administrative and policy decision should be vested in. The conduct of the certification process, upon which the accreditation decision will be based, is left to the discretion of the accrediting authority. Further delegation of accrediting authority could lead to non-uniformity of policy application within CIA.
3. Data Owners should have input to the accreditation process	Whereas accreditation authorities should take cognizance of the requirements of data owners, giving them explicit roles could lead to administrative problems and policy conflicts, particularly if lines of authority cross agency boundaries. We must avoid creating authority without responsibility. The data owner already affects the accreditation by the classification, compartmentation and handling caveats he affixes to the data.

CONFIDENTIAL

4. CIA DD's should be able to redelegate accreditation authority.	The real burden of both accreditation and reaccreditation will be imposed on those who do the certification. As stated above, it is within the discretion of the accredting authority as to who does this. Accreditation is a policy decision based on an assessment of the risk derivied from the certification process. There is no reason to separate the level of responsibility required for original accreditation from that of reaccreditation.
5. DCID should state more strongly that accreditation is an assumption of risk.	CIA should be tasked to propose specific language designed to accomplish this. I think it is clear in the language of the draft.
6. Objection to mandating of use of EPL products "where feasible". Argues accrediting authority should be able to evaluate and in effect substitute products not on EPL.	I believe that the draft makes clear that Accreditors accredit systems not products and permits policy objectives to be accomplished by means other than the use of EPL listed products. The whole thrust of the Center and the EPL is to provide the incentive for industry to provide trusted products. The balance in the language now in the draft concerning the use of EPL products has been carefully worked out. We should not risk upsetting the apple cart on this point now.
7. Interim approval to operate should not be limited to one year.	Strongly disageree. Security should be built in from the beginning and provided at all stages of development. Although the security environment and architecture may change over a multi-year development cycle, accreditation status should be fixed within one year of IOC and adjusted as required over the devlopment period.

8. Editorial.	Agree.
9. Media containers should be labelled with highest level of data "which can be" placed upon the medium.	I think Lara misconstrued the intent of the comment. Whereas the draft requires labelling at the highest level ever actually stored on the media, the CIA comment seems to want to require labelling with the high water mark of the system on which the media was used. There are problems with a literal application of the draft language. These were addressed and resolved in the course of the drafting of the magnetic media labeling standard. Perhaps the problem would be better addressed by incorporating this standard in the DCID by reference. (The labeling standard should be added to list of references in Appendix "A")
10. Interprets draft to require manual review of all output from dedicated or system high systems.	While this a misinterpretation of the intent of the draft, the present language is subject to such a misinterpretation and should be revised.

CONFIDENTIAL